ESTHER DYSON'S MONTHLY REPORT

Release 1.0®

VOLUME 20, NO. 2 | 19 FEBRUARY 2002 | www.edventure.com

Bringing it all Together: Infrastructure for Collaboration

BY KEVIN WERBACH

Collaboration is one of those "C" words in technology that seem simple until you examine them. (Others are communications and community.) Just what it means for a group of users to work collaboratively is open to debate, but at least there is a relatively well-defined collaboration software category, covering functions such as shared whiteboards, document markup, online meetings, workflow and discussion groups.

Before users can engage in these activities, however, they must be able to get themselves and their data into shared environments, and they must do so securely. The proliferation of Internet-connected users makes collaboration more important than ever, but it also pushes collaborative business activities beyond the protected environment of the corporate network. Traditional mechanisms break down under these circumstances. The companies attacking the security and data-sharing problems around collaborative business rarely call themselves collaboration vendors. Yet what they do is an essential underpinning for effective collaborative business processes.

Collaboration involves shared context between users. That context may be embodied in a conference call, a document, a report from the customer relationship management application, or a set of PowerPoint slides. Supporting shared context when users are on different networks or in different locations is tricky. . . but those are the scenarios where online collaboration adds the most value. Most users today share information and documents with co-workers and partners using email attachments, which are neither secure nor manageable. There must be a better way.

{ *continued on page 2* }

INSIDE

BRINGING IT ALL TOGETHER 1
  Beyond the LAN's End 2
    The time is now
    Virtualizing the infrastructure
  Secure Information-Sharing 5
    Box: P2P security
    Endeavors Technology
    XDegrees
    Groove
    Box: Intraspect and Interwise
  Plug-and-Play Extranets 11
    Existing options
    Application-level security
    Neoteris
    SafeWeb
  Security + Groupware = ??? 16
ACROSS THE BROADBAND DIVIDE 17
    Broadband matters
    Is the glass half full?
    The longer view
    Where are we going?
  Resources & Contact Information 22
  Calendar of High-Tech Events 23

Visit www.edventure.com/pcforum for updates on PC Forum speakers and sessions. See you in Scottsdale!

edventure
The conversation starts here.

The first issue is how you get into a collaborative environment in the first place. The resources users need are generally inside the corporate network, behind the firewall, but increasingly those users connect from the outside. Security and data-sharing functions become critical. The traditional ways to overcome the barriers in the middle are expensive, difficult to support and not scalable, which is why their penetration has been limited. Two new approaches are distributed collaboration platforms and plug-and-play extranet appliances. These solutions promise to tie people on the outside to the resources on the inside more or less transparently.

Beyond the LAN's End

The time is now

The first question businesses asked about the Internet was, "What is it?" The second was, "How do we go online?" The third is, "How do we do something useful with it?" With the focus shifted from digital transcendence to cold, hard return on investment, that final question is now being asked seriously.

The challenge is more than how to get data on the corporate Website, the employee portal, or the supply-chain extranet. Taking those as a given, companies must figure out how to enhance real-world projects and other activities. That involves focusing on the human dimensions of knowledge (SEE **RELEASE 1.0**, JUNE 2001) and using new text-processing tools to combat information overload (SEE **RELEASE 1.0**, DECEMBER 2001). Secure collaboration and information-sharing is another aspect.

Tools such as Microsoft's NetMeeting and Lotus' SameTime and QuickPlace share video and audio of meeting participants and offer tools such as shared whiteboards. Smaller companies offer virtual meetings (WebEx, GoToMyPC and Placeware), threaded discussions (QuickTopic) and shared workspaces (IntraLinks).

Tighter digital links between co-workers, customers and partners make collaboration an increasingly significant function. Whether

Release 1.0® (ISSN 1047-935X) is published monthly except for a combined July/August issue by EDventure Holdings Inc., 104 Fifth Avenue, New York, NY 10011-6987; 1 (212) 924-8800; fax, 1 (212) 924-0240; www.edventure.com. It covers software, the Internet, e-commerce, convergence, online services, Web applications, technology policy, groupware, data networking, streaming media, enterprise applications, wireless communications, intellectual property and other unpredictable topics.

EDITOR-IN-CHIEF: Esther Dyson (edyson@edventure.com)

PUBLISHER: Daphne Kis (daphne@edventure.com)

EDITOR: Kevin Werbach (kevin@edventure.com)

SYSTEMS DIRECTOR: Scott Giering (scott@edventure.com)

CIRCULATION MANAGER: Natasha Felshman (natasha@edventure.com)

OFFICE MANAGER: Bill Demeritt (bill@edventure.com)

EXECUTIVE ASSISTANT: Irene Lawrence (irene@edventure.com)

CONSULTING EDITOR: Bill Kutik (bill@kutik.com)

Copyright © 2002, EDventure Holdings Inc. All rights reserved. No material in this publication may be reproduced without written permission; however, we gladly arrange for reprints, bulk orders or site licenses. Subscriptions cost $795 per year in the US, Canada and Mexico; $850 overseas.

the goal is designing a car or negotiating a merger, traditional tools such as phone, mail, fax and face-to-face meetings are becoming too slow and inflexible for the pace of modern global business. And there are other influences at work as well. The meeting services, in particular, have enjoyed strong demand since September 11, as many businesspeople who would otherwise fly to in-person meetings are staying home because of corporate travel restrictions or security concerns.

If the participants are down the hall from one another, collaboration is fairly straightforward. . . though it may still be hard to manage, control, or measure. The pervasive local-area networks (LANs), Websites and other tools built during the "how do we go online" phase of Internet development, augmented with server-based groupware platforms if desired, offer an array of collaboration mechanisms.

Things get dicey when different members of the team want to participate from home, from the sales office in Paris, from a hotel room in Dallas or over a wireless connection at Starbucks. And they become particularly challenging when those seeking to collaborate work in separate organizations: for example, an accountant from Andersen, a managing accounting partner in Chicago, a lawyer from Vinson & Elkins, surely some investment bankers, a couple of managers and a senior executive who is too important to be bothered with details. You can get online from virtually anywhere, it seems, but if you want to do collaborative work outside the corporate perimeter you must either sacrifice functionality or manage security more carefully.

Such situations are becoming the norm. Massive investment in enterprise resource planning, online procurement, B2B integration and supply-chain management mean that companies' internal and external processes are interconnected. Kittu Kolluri, ceo of virtual extranet appliance vendor Neoteris (SEE PAGE 13), admits that, "A company like Neoteris would have been a solution looking for a problem to solve two years back. Today, the timing is right, because it's a very real pain point."

There's an important conceptual leap to make here. Remote access to email or salesforce automation systems isn't usually thought of as collaboration. . . but it should be. Collaboration is more than groupware and knowledge management (which inevitably bring to mind Lotus Notes). It's a way to get work done involving groups of people, who may or may not be inside the firewall. Call it collaboration, call it information-sharing, call it secure access to network resources, but it's something almost every business needs today.

Virtualizing the infrastructure

In terms of technology, the key step in moving beyond server-based groupware and realtime communications to anywhere, anytime collaboration is to virtualize the network infrastructure. We assume that, simply because everyone is on the single platform of the Internet, people can work together smoothly. Unfortunately, the Net universally supports only least-common-denominator services such as email, instant messaging and Web browsing. Numerous blockages and bottlenecks keep data from flowing freely. Some are even intentional: Many companies have firewalls at the boundaries of their networks for security.

A firewall allows only certain types of traffic to pass through. If an employee tries to connect to the corporate customer relationship management application from home, he or she will probably be stopped by the corporate firewall. Keeping corporate resources secure is certainly important, but the proliferation of firewalls has the effect of balkanizing the Internet.

In theory anyone can talk to anyone else, but in practice they can't say very much to each other. Getting access to anything behind the firewall – the email server, the sales-force automation system, the shared file directory for your current project – requires additional software or hardware. Unfortunately, deploying that new layer of infrastructure can cause serious integration or deployment issues. The missing link for collaborative business, therefore, is to make this balkanized landscape look like one local network again, at least for the documents and activities in your sphere of collaboration. "What we may be looking at here is the next generation of secure connectivity," proclaims XDegrees ceo Michael Tanne (SEE PAGE 8).

Various companies do some form of storage virtualization, decoupling files from their physical location. They make the barriers on the Internet go away by substituting their own virtual directories. This is a core feature and important reason for the success of peer-to-peer (P2P) file-trading applications such as Napster, Gnutella and Morpheus. You don't need to know where a song or other file is stored to download it through one of these systems; you just need to know what it's called.

Outside the P2P file-trading context, Novell's iFolder automatically synchronizes local files in a specified directory to a server, making them universally available. Mangosoft's Mangomind automatically turns desktop hard drives on a LAN into file caches, and retrieves files from the closest user while displaying them through a standard directory. And distributed collaboration platforms such as Groove, XDegrees and Endeavors (SEE PAGE 6) all incorporate some form of virtualization.

Freeing a user from having to know where a file is stored is a start. However, the more common business challenge arises when users know where files and applications are located, but can't get to them. This is where security becomes a serious barrier. Comprehensive systems for managing security policies (SEE **RELEASE 1.0**, FEBRUARY 2001) or identities generally focus on those already inside the network. Giving all outside users full access to internal corporate resources would be foolish. The question then becomes how to distinguish between friends and strangers, and to determine what should be accessible to which friends in a specific situation.

The most common method today is to build special infrastructure to go through or around the firewalls, such as virtual private networks (VPNs) or extranets. Unfortunately, the overhead of that infrastructure limits the number of users it can realistically and cost-effectively support (SEE PAGE 12). Moreover, these solutions reinforce the balkanization of the Net, rather than overcoming it.

Below, we describe two superior approaches. One is to deploy software that layers security and firewall navigation on top of the existing environment. The best way to do so is to add intelligence to the edges of the network, with virtual file systems and firewall-navigation plumbing to overcome Internet balkanization transparently for authenticated users. The other mechanism is to add a new layer of hardware to corporate networks, through appliances that securely proxy remote access to internal files and applications. Unlike VPNs, these appliances are transparent to the user and require nothing more than a Web browser and a password for external connections.

Secure Distributed Information-Sharing

When you think about it, distributed or P2P collaboration makes perfect sense. Collaboration is a way to bring together dispersed *people* so that they can work on a single project or activity. Centralizing intelligence on a server or in a file repository, without giving the people involved tools to tap into that intelligence resource, doesn't address the real problem. As we stated in analyzing the related domain of knowledge management (SEE **RELEASE 1.0**, JUNE 2001), systems need to track what users do, instead of the reverse. If users are spread across different locations and companies, give each of them the power to participate fully in the collaborative enterprise.

Below, we describe three infrastructure solutions for secure distributed information-sharing. Endeavors Technology's Magi and XDegrees both provide platforms for secure access to network resources using a P2P architecture. Groove offers a more heavyweight client that in addition to creating a P2P collaboration environment provides tools and development hooks.

Endeavors Technology: Do you believe in Magi?

Magi, Endeavors Technology's distributed collaboration platform, began as a DARPA-funded project led by cto Greg Bolcer at the University of California at Irvine. Bolcer was a prime mover behind Web distributed authoring and versioning (WebDAV), an Internet Engineering Task Force standard for distributed document authoring and workflow. He and his team worked to develop technology for distributed collaboration that levered Web standards, initially as an open-source project.

In 2000, Endeavors was acquired by Tadpole Technology, a British wireless solutions company. Tadpole was developing field systems to connect utility workers and was looking for a lightweight cross-platform workflow system, when it came across the Endeavors project. "I said, 'I don't know what the killer app for this technology is. But I think what you've got here is good enough to build on, if we focus on some initial markets'," says Tadpole ceo Bernard Hulme.

ENDEAVORS INFO

Headquarters: Irvine, CA
Founded: 1999
Employees: 40
Funding: $4 million from DARPA;
  approximately $10 million so far
  from parent Tadpole Technology
URL: www.endeavors.com

Tadpole paid $3.3 million for Endeavors and kept it as an independent subsidiary with its own options pool. The relationship with a public company insulates Endeavors from venture capital vicissitudes, while allowing it to maintain the structure of a startup. The company continues to support the open-source version, but is concentrating its efforts on an enterprise version of the platform, now in version 3.0.

"Basically, Magi is an abstraction layer next to the Web," explains Hulme, who serves as chairman of Endeavors. It puts a Web server onto every device and uses WebDAV to support two-way connections to documents through a peer-to-peer network. With the Magi desktop application running in the background, users can drop files into shared folders (either public or subject to access controls) and make them securely accessible to others. For example, salespeople could update forecasts on a single Excel spreadsheet, instead of emailing around several versions that an administrator has to merge together for the monthly sales meeting.

With WebDAV-enabled applications (including Microsoft Office and Adobe Acrobat), users can open files directly and have them automatically versioned and

P2P SECURITY

Ironically, the way to make collaboration more secure is to make it more distributed.

P2P technologies have a reputation of causing security problems. This is partly because P2P remains associated with Napster and unauthorized sharing of copyrighted content, and partly because P2P architectures greatly multiply the number of points with full access to an application. If a Web browser is just a dumb client, the only important point to secure is the smart server at the other end of the connection. Files can be secured in a single central vault. If, on the other hand, every end-user is an active participant in distributed applications and services, one rogue participant can compromise the entire network. Information is distributed everywhere, creating many new places for security to break down.

While it's true that insecure P2P applications pose a significant security risk, this formulation is backwards. P2P means putting more functionality at each node of the network. That, in turn, means that each node can take responsibility for security. With a secure P2P system, security is no longer a single point of failure. It can be built into the very fabric of the network. And it can be implemented at the object level, granting access only to specific resources based on granular policies.

Endeavors' Magi, Groove and XDegrees all provide such a comprehensive distributed security environment. Their desktop software secures data locally and also encrypts everything that passes over the wire. All of them provide full-blown certificate-based authentication, key-management and access controls.

These security features are part of the distributed platform rather than separate infrastructure that must be integrated. Consequently, they are transparent to end-users. Robust security is part of the plumbing that the end-user nodes that make up the distributed network handle by default, unlike the client-server browser model that expects security to come from the center.

updated for other users in the group. Non-WebDAV applications, such as AutoCAD, are also supported in the latest release through the Magi browser, which serves as a proxy for the remote application. "The beauty of it is that there's no programming between the environment, which is Magi, and all the applications you're already using," notes Hulme. In this way, he distinguishes Magi from competitors such as Groove, which provide open component interfaces but require applications to be integrated with their environments.

Magi includes its own simple public key infrastructure, a private domain name server to virtualize resource locations and a connection broker to allow connections across firewalls consistent with existing corporate access policies. Because it is based on Java and a Web architecture, Magi can run on both PCs and handheld devices. The latter are particularly important for mobile applications such as field sales and field service. It supports search and discovery across the virtual network, making it possible to find shared content on desktop PCs or other end-user devices.

Endeavors charges in the range of $200-$300 per user for 1,000 seats. (Each seat represents an individual, who may have several devices.) It has four paying customers and several others evaluating the software, ranging from telcos to car manufacturers. The ideal customer is someone with a distributed workforce engaged in highly collaborative activities such as product design or clinical trials for pharmaceutical companies, but in a situation where the information must be highly secure.

XDegrees: getting warmed up

XDegrees was part of our report on peer-to-peer infrastructure (SEE **RELEASE 1.0**, DECEMBER 2000). The startup built a framework for decentralized Web applications, based on a novel distributed namespace. Though XDegrees may have originally hoped others would take its platform and build on top of it, the company found it could win more customers by providing a set of functions directly. The direction it went ties directly into the themes we've been exploring.

"XDegrees is focused on the ability to rapidly deploy a system with very low management costs that lets you access data regardless of where it's located," explains ceo Michael Tanne. Email is a good mechanism for simple, ad hoc communications, but it's not secure or reliable enough for important collaborative business activities. "You wouldn't use your inbox as the place to store all of your bill of materials for your production run," says Tanne.

The core of XDegrees' system is a namespace for distributed resources, called extensible resource name system (XRNS). Unlike a traditional directory, XRNS overlaps with the Internet's domain name system and uses ordinary URLs. Customers create a sub-domain for XRNS, such as share.edventure.com. URLs outside that subdomain work normally, but files below it (such as share.edventure.com/contract.doc) map to virtual locations rather than physical directories.

When a user running XDegrees software requests a file with an XRNS address, the request goes to an XRNS nameserver which determines the location of desired documents. The system automatically caches, synchronizes and tracks versions of files, so that it returns the right file. "Anyone on the Net who has the right authority can simply follow a link, which queries the nameserver to get the resource," says Tanne.

So if you're logging in from a hotel, all you do is find a URL for the material you want, which may be sent to you by email, pushed to you via a subscription to a virtual folder, or located through a full-text search. Requesting the file pulls it from the most efficient location, which might be somewhere across the network or might be a local cache on your hard drive. XDegrees has developed smart caching and downloading algorithms to support situations where connectivity is unreliable. Users can take advantage of XDegrees' system with only a browser (based on WebDAV), though they need client software to be a source of documents or for offline access.

XDegrees has 18 potential or paying customers in its pipeline, and it is finalizing a significant OEM deal with a managed service provider. One XDegrees customer is a major professional services firm whose employees spend much of their time on-site at clients as part of their engagements. The employees can't get into their corporate intranet because they are logging in from inside another company's network. XDegrees gives them a better way to share files and collaborate around documents.

Another potential customer that is beginning trials with XDegrees is using the software for its several thousand person finance group, spread across more than a dozen offices. They need to move sensitive files around the company, but doing so through email attachments leads to network performance issues (with large files) and massive confusion due to multiple copies of documents.

Groove and its new collaborator

Groove is a little bit of everything. In addition to being a high-profile bet on P2P connections and a mechanism for distributed knowledge management (SEE **RELEASE 1.0**, JUNE 2001), it's a perfect example of a distributed secure collaboration platform. In the past, we've described how Groove's shared spaces offer a flexible environment for users to engage in collaborative work activities (SEE **RELEASE 1.0**, NOVEMBER 2000). Those activities are possible because Groove does the heavy lifting of virtualizing network infrastructure and guaranteeing security as part of its platform.

In October, Groove announced a $54-million funding round, including $51 million from Microsoft. Since Groove founder Ray Ozzie created Lotus Notes, and Microsoft's Exchange is Notes' largest and fiercest competitor, the deal was surprising. But it makes sense when you think about it. Microsoft's stronghold is on the desktop, so it benefits from the success of P2P tools such as Groove that empower desktop and laptop machines to perform richer functions.

At a more specific level, Microsoft sees the collaboration market as the primary business motivation for the deal. Microsoft group vice president Jeff Raikes explained the connection at the time: "It's our feeling here at Microsoft that this is going to be a very exciting decade for the creation of a lot of value from online collaboration and online workspaces." Raikes tied this trend directly to developments in connectivity such as broadband and more realtime systems.

From Groove's side, there's the obvious benefit of having Microsoft as a partner rather than a competitor. Groove's component-based vision also harmonizes with Microsoft's .Net and Web-services vision (SEE **RELEASE 1.0**, OCTOBER 2001). Groove has demonstrated integration with Microsoft's instant messaging client and its .Net My

ENTERPRISE-WIDE COLLABORATION: INTRASPECT AND INTERWISE

As distributed forms of work become more common, collaboration is growing beyond internal niches such as product design and becoming a core software infrastructure element for many enterprises. Companies such as Intraspect and Interwise with broad collaboration offerings are increasing their enterprise-wide deployments. Those two vendors are among the larger pure-play online collaboration companies. They make an interesting case study because they see the same trends from different vantage points: one coming from knowledge management, the other from e-learning.

According to Jim Pflaging, ceo of collaboration software vendor Intraspect, "From last fall forward, we saw that many companies had enterprise collaboration in their budgets," whereas before Intraspect had to sell most customers on the idea of collaboration before pitching its product. Pflaging sees this as evidence the space is maturing, with solid case studies and a timely promise of improved efficiency helping woo conservative enterprises.

Intraspect offers a deep set of tools that integrate shared workrooms with email, knowledge management and information discovery. It has more than 200 customers, primarily in financial services, marketing services and high-tech. Intraspect's vision for collaboration parallels the new wave of bottom-up knowledge-management solutions (SEE **RELEASE 1.0**, JUNE 2001). As Pflaging observes, "People have realized the missing link is, how do you capture the day to day interactions that are going on among people? And you want those interactions to be mined across the enterprise."

Pflaging sees an opportunity at the intersection of collaboration, knowledge management, enterprise portals and content management, the market spaces that concern employees' interaction with unstructured or semi-structured data. Increasingly, he says, Intraspect is seen as a companion to customer relationship management (CRM) or enterprise portal deployments, which organize information but don't necessarily tie together the relevant people inside and outside the company. In CRM, for example, the goal is for the world to revolve around the customer (SEE **RELEASE 1.0**, SEPTEMBER 1998). "I think people realize that where CRM is letting them down is that there's more to managing a customer relationship than providing all the analytics," says Pflaging.

Where Intraspect concentrates on asynchronous collaboration and workflow, Interwise specializes in collaborative live communication. Interwise began as an e-learning company. Its original technology was developed by a group of Israelis who had previously done similar work for the Israeli air force under the direction of Frank Zvi, an ex-fighter pilot who is now Interwise's ceo. Though the company had some success offering online classrooms for corporate training, it found that customers wanted to use its interactive broadcast capabilities for a broader range of functions. So Interwise re-built itself to support the entire spectrum of live enterprise collaboration.

In practice, that means offering five modes ranging from mentoring (one-on-one) to broadcasting (one-way, one-to-many), with meetings, classrooms and seminars in between. All of them use streaming audio and video based on Interwise's own technology to support realtime interaction among participants, integrated with shared documents, instant messages, polls and other features. They differ in the interaction rules and tools they offer. For example, in a meeting everyone can talk, but in a classroom participants must "raise their hand" and be called on before speaking. Zvi says Interwise designed its interfaces using subtle techniques derived from experience with airplane cockpits, avoiding information overload by helping users quickly spot what's important on the screen.

Zvi says that many enterprises are spending large amounts of money on live collaboration solutions today, but it's divided up into unrelated departmental deployments. One system may be handling online sales meetings, one may be supporting the ceo's company-wide quarterly updates, while another supports e-learning. "Having different systems broadcast on your intranet is IT's worst nightmare," says Zvi. Interwise replaces these with one platform. It has more than 300 customers, with a strong base in software companies such as SAP and Microsoft.

To support users distributed across an enterprise, both inside and outside the firewall, Interwise employs a distributed architecture for its streaming media servers. It automatically clusters users and multicasts streams to cut down on redundant transmissions across the network. It also operates its own network of servers on the public Internet, so that employees can participate in the live broadcasts and meetings from outside the corporate network. Interwise offers both Windows and Java versions of its client software; later this year it will also allow users to tap into meetings via mobile phone.

Services alerts to segue smoothly from ad hoc collaboration through email attachments and shared whiteboards into the integrated Groove environment.

In the prototype, clicking on a “Groove” button in the Windows Messenger taskbar automatically creates a Groove shared space, fires off emails inviting the participants to join, pastes the transcript of the instant messaging conversation into the Groove chat log and pulls the file attachments into Groove’s persistent XML-based file storage. Now everyone has access to the materials locally and securely, and they can continue their interaction through Groove. “This is a beautiful thing,” says Groove’s Andrew Mahon. In addition to the technical integration, partnering with Microsoft guarantees Groove distribution and screen real estate on one of the two dominant instant-messaging platforms.

Plug-and-Play Extranets

Existing secure networking options

Secure communications become important when people engage in valuable activities over networks, especially when those activities require rapidly changing connections between dispersed individuals from many organizations. Few companies would pay to ensure the security of their customer email newsletters, but equally few would feel comfortable without a mechanism to protect communications with partners about potential important transactions.

There are several mechanisms to make computer networks secure. The most blunt is to use dedicated private lines, so that no one else’s traffic flows over the same physical network. Most networks ran on private lines in the days before the Internet. Large organizations and those requiring extreme security, including the military, financial institutions and multi-national corporations, still use private lines extensively. The downside of private lines is that they are expensive and hard to maintain, because a separate point-to-point connection must be established and dedicated to each link. For most traffic, the Internet’s many-to-many shared infrastructure has completely replaced private lines. But the Internet has no built-in security.

The first hybrid of the Internet and security is the VPN. A VPN sends traffic over the Internet through an encrypted tunnel, generally using the IPsec protocol. Since every packet is encrypted, anyone looking at the traffic will see only gibberish. Software on the both ends of the connection creates the equivalent of a private line – a secure point-to-point connection – on top of the public Internet.

Unfortunately, VPNs have their own failings. They require software or hardware on the user side that modifies the local Internet protocol stack. Deploying and maintaining this software is challenging, especially for large numbers of users. Explains Neoteris ceo Kittu Kolluri (SEE BELOW), "To look at it from a philosophical point of view, when the rest of the world has moved over to a universal client model, VPNs are stuck in a client-server model."

Moreover, because VPNs secure data through network layer tunnels, the protection is all-or-nothing. A compromised VPN-enabled PC can provide full access to internal systems. In 2000, for example, an intruder gained access to Microsoft source code by putting a worm on a Microsoft employee's laptop. Says Kolluri: "You're building a moat around the company, but you've provided a tunnel into it. You've extended the boundaries of a LAN to a machine that you haven't secured."

Instead of point-to-point VPNs, some companies have deployed extranets, which are specially built secure networks using Internet protocols. Extranets provide security at the application or resource level. They are often used for partner networks, where a group of companies wants to connect securely with one another to exchange information, but not to provide full access to their internal networks.

Unfortunately, extranets are expensive. They must be specially deployed for the network of partners and the specific files or applications. Says Kolluri: "Extranets are not something you can go to Fry's or CompUSA to buy." In most cases, companies must invest in redundant servers and licenses to run separate instances of their enterprise applications on the extranet and on their intranet.

Application-level security without the hassle

The alternative to extranets and VPNs is to do security at the application level on existing networks. Instead of encrypting every packet, this approach looks at the traffic between end-users and specific applications or files, and allows or disallows access in a granular way. Unlike extranets, it doesn't require a whole new network. Companies such as Endeavors and XDegrees (SEE ABOVE) do this with software. The same approach can also be applied to hardware, through server appliances.

The benefit of such appliances is that they create plug-and-play virtual extranets. From the end-user's perspective, connections from anywhere to internal directories and applications are secure without any special software. From the company's perspective, the solution looks like a VPN, because it doesn't need the redundant servers, special networking configurations and other elements of an extranet. "A browser is an interface that's going to travel across platforms," says SafeWeb chairman Stephen Hsu (SEE BELOW). "The challenge is to develop a VPN-like capability or an extranet-like capability, but do it through an ordinary Web browser."

Neoteris and SafeWeb do so with devices in the middle of the traffic stream that read all packets going through. In other words, users connect to the box, and the box connects securely to internal systems. The appliance functions as a reverse proxy, transparently transforming URLs and other external resource calls. The connections are secured using SSL, the standard protocol for e-commerce transactions, which offers the same level of encryption as the lower-level IPsec protocol that VPNs employ.

Reverse proxies are part of existing Web servers such as the one from iPlanet, the Sun/Netscape joint venture. However, they don't work terribly well for content other than plain HTML. Parsing Java, Javascript and other traffic to identify and rewrite external resource calls is tricky. The differences among browsers mean that even when an application has a Web front-end, it may render in a number of different ways using Javascript and stylesheets.

Neoteris: the new world of secure access

Neoteris is the first startup out of the gate with an instant virtual extranet appliance. "Our appliance enables instant secure access to selected corporate network resources for employees and partners, from any Web browser," explains ceo Kittu Kolluri. Kolluri was a senior vp at Healtheon, Netscape co-founder Jim Clark's ambitious (and not fully successful) effort to automate much of the health care industry. Clark and former Netscape ceo Jim Barksdale are both investors in Neoteris, giving the startup significant credibility.

NEOTERIS INFO

Headquarters: Mountain View, CA
Founded: May 2000
Employees: 40
Funding: $20 million from New Enterprise Associates, Jim Clark and The Barksdale Group
URL: www.neoteris.com

Kolluri says the inspiration for Neoteris came directly from his experience at Healtheon. Like many companies, Healtheon struggled with the support obligations of remote-access lines and VPNs to give its employees access to internal corporate resources. The most successful initiative was Web-based mail, because employees could get to it through any browser. But mail was only one function employees wanted. Recalls Kolluri: "When one of our founders came up with the notion of repurposing server-based browsing technology to enable application-layer secure access, I literally grabbed him and said, 'that's it, man!'"

Neoteris' appliances sit directly behind the corporate firewall. "No user on the outside ever directly connects to a server on the inside. It all goes through our box," explains Kolluri. From any Web browser, a user can log in and go directly to whatever resources he or she has access to. Administrators can configure access controls for the Neoteris box with a Web-based interface. Neoteris has had security experts certify its security implementation, which it claims is at least as effective as a VPN.

The company sells one version of its box designed for employee remote access to corporate applications and files, and another version for information exchange between partners. The main difference is that the partner appliance includes more sophisticated access controls and workflow to manage large numbers of users coming from different points. Pricing ranges from $15,000 to $65,000 for the employee access device, and $30,000 to $100,000 for the partner access device.

One of Neoteris' pilot customers also had a VPN. Some of the employees using the VPN, however, were customers of Excite@Home's cable modem service, and when Excite@Home shut down and moved its customers to AT&T Broadband, those employees could no longer get into the corporate network remotely. The pilot customer turned to the Neoteris box as an alternative.

Neoteris doesn't see itself totally displacing VPNs, because it can't support client-server applications that don't have a Web or Telnet front-end. For the minority of employees who need to use such applications remotely, Kolluri says, VPNs still make sense. But the bulk of employees and partners can be served more effectively by the Neoteris solution. Neoteris has more than twenty customers evaluating or using its product, a majority of whom are paying.

SafeWeb: from Internet anonymity to enterprise security

SafeWeb took an interesting route to application-level security appliances. The company's initial offering was an anonymous Web surfing service, launched in October 2000. The free, advertising-supported service processed as many as 4 million pages per day during its peak. It worked by relaying requests through its own servers, which stripped off identifying information. Website requests seemed to originate from SafeWeb's servers, instead of the actual origin user.

The service particularly appealed to individuals in countries that restricted freedom of speech, because it enabled them to anonymously communicate with the outside world. Many countries, including China, have deployed filtering servers on their Internet backbones, automatically screening out content from the rest of the world that they deem improper, and monitoring outgoing traffic. Those countries blocked SafeWeb's service by blocking the company's IP address. In response, SafeWeb created TriangleBoy, a P2P application that volunteers deploy on their PCs. This created an additional layer of intermediation, with many intermediary sites, thus circumventing the filtering mechanisms.

SAFEWEB INFO

Headquarters: Emeryville, CA
Founded: April 2000
Employees: 25
Funding: $9 million from In-Q-Tel, Chilton Investments and Kingdon Capital Partners
URL: www.safeweb.com

The privacy and anti-censorship features of SafeWeb's system won it an investment from In-Q-Tel, the CIA's venture capital fund, and a relationship with the Voice of America. However, the company wasn't able to generate enough revenue from advertising and subscriptions to cover the bandwidth costs of the service. So in November, SafeWeb shut down its free service. The Voice of America will continue to operate a licensed version to provide anonymous surfing to those subject to government censorship. SafeWeb also licensed the technology to PrivaSec, which offers a fee-based version.

Like many startups, SafeWeb is now following the money and pursuing corporate customers. It has taken the work it did for the consumer service and turned it into an enterprise product, using a similar approach to Neoteris. SafeWeb's Tsunami appliance can be deployed quickly to provide a secure gateway for remote access to email, file-sharing and Web applications.

The new product is designed for security rather than anonymity (corporate IT departments *want* to track who is using their network), but it uses the same basic proxying mechanism as the consumer service. "What we're basically selling is SafeWeb in a box," says chairman and co-founder Hsu, who is on leave from his position as a professor of theoretical physics at the University of Oregon.

Where consumers connected to SafeWeb's own servers and reflected out to other sites, Tsunami customers reflect off a box co-located at their own company, which reflects them to internal resources. "The advantage of this way of doing things is that it gives you finer control over what's going on," explains Hsu. Administrators can control what resources users outside the firewall can manipulate, with integrated reporting, in contrast to VPNs which deliver undifferentiated encrypted packets.

Hsu sees the possibility down the road for SafeWeb's appliances to brand into other B2B integration and collaboration functions. He explains: "When you're doing application-level proxying, what you're really doing is modifying code on the box as it goes out. If you can modify code, it is straightforward to modify data as well." The security device providing the proxying has the intelligence to know how data is flowing between applications.

Hsu believes scalability is the company's key advantage against Neoteris and other competitors. SafeWeb can support large numbers of users with high reliability, because it has experience doing so with its consumer service. That service handled 1.5 billion secure transactions in 2001, with up to 100,000 simultaneous users.

Security + Groupware = ???

Is a mechanism that allows employees within and across companies to exchange files and work collaboratively in a secure and reliable manner a security solution or a groupware solution? It depends. And in the end, it hardly matters. As we noted a year ago, security isn't an all-or-nothing concept; it's an evolving set of business policies (SEE **RELEASE 1.0**, FEBRUARY 2001). Security and data-sharing are means, not ends. They are mechanisms to make it possible for people to work online in a collaborative, distributed manner.

Most of the products we describe above can be licensed for integration into more comprehensive systems. Security and data-sharing are plumbing, and as such they are most useful when users don't even know they are there. Furthermore, if application developers can partner with distributed platform providers, they can enable secure cross-organizational uses of their software without having to build everything themselves.

The distributed secure collaboration solutions extend the power of the Internet further into business. Just as the Web freed users from having to run special-purpose software for every type of file, transparent security and data-sharing frees them from having to worry about how to connect up the co-workers, partners and resources they need to work with. The browser isn't the application users care about; what they want is what they can interact with through the browser window. Collaboration takes the power of the browser, which is largely one-way, and helps expand it to two-way or any-way connections. ■ **R 1.0**

Across the Broadband Divide

BY KEVIN WERBACH

"The widespread deployment of broadband infrastructure has become the central communications policy objective today," declared US Federal Communications Commission Chairman Michael Powell in October. It's hard to disagree. Policymakers, commentators across the political spectrum and leaders of powerful technology companies, are all talking about broadband. And they are saying the same thing: broadband isn't happening fast enough (SEE **RELEASE 1.0**, JULY/AUGUST 2001). *(Michael Powell and leaders of major telecommunications and Internet companies will discuss the broadband bottleneck next month at PC Forum.)*

Things aren't as bad as everyone thinks. Universal broadband was never going to happen overnight. After all, eight years after the first graphical Web browser, we still have only 50-percent Internet penetration in the US. Looking to the future, though, the broadband situation is *worse* than it seems. There is no quick fix for the broadband bottleneck. The solutions being bandied about don't get to the real issues, and they will raise expectations unrealistically. We need a long-term broadband strategy.

This just in! Broadband matters

Three years ago, we looked at still-nascent cable modem and digital subscriber line (DSL) services and sounded the alarm about a perversion of the Internet's fundamentally open architecture (SEE **RELEASE 1.0**, FEBRUARY 1999). Internet 2.0 – a broadband, always-on, converged network – was taking shape. The companies building on-ramps to that network wanted to control what content could flow over it and who could provide services to end-users. Their vision would have constrained the Net's competitive and innovative dynamism.

The landscape has changed a great deal since then, with Excite@Home and several independent DSL service providers going bankrupt and the Internet bubble bursting. What hasn't changed is that Internet 2.0 is still out in the future somewhere. A number of factors have held up employment of the crucial enabler – broadband last-mile connectivity. Cable companies shot themselves in the foot by demanding exclusive control instead of leveraging the talents of independent service providers.

When the debate about open access to high-speed cable Internet services began, policy makers felt they could safely avoid the hard questions it raised. After all, broadband services had tiny subscriber levels. The big story then was still the race toward more ubiquitous Internet penetration. At the height of the dotcom boom, it seemed that broadband was destined to happen, like so many other epochal transformations wrought by technology. Governments felt their main role was to stay out of the way of the onrushing train of private investment.

The talk today is all about what government can and should do to promote broadband deployment. The FCC under Michael Powell has launched proceedings to consider whether the FCC could spur greater investment in broadband through deregulatory steps. Supporters and opponents of the so-called Tauzin-Dingell bill, which would deregulate certain activities of incumbent local phone companies, spent millions of dollars on TV commercials in Washington, DC, last year. The bill didn't even make it to a vote before Congress adjourned. Meanwhile, TechNet, the powerful Internet industry lobbying organization, announced in January that broadband was its top priority. It released a report (SEE RESOURCES SECTION) calling on the government to promote broadband deployment more forcefully, and to eliminate legal and regulatory barriers.

For all the energy being devoted to the topic of broadband, the proposals being advanced are strangely short-sighted. If broadband truly involves massive startup investments that no sane company would undertake without a large, guaranteed revenue stream and control over applications, how could it be so important? At $50/month for about half a megabit per second downstream, today's cable modem and DSL offerings are hardly going to transform the US economy. TechNet's goal of 100 million households with 100 megabit connections in ten years is inspiring, but does anyone really believe earnest government well-wishing will get us there?

Is the glass half full?

We'd all love to see copious amounts of bandwidth ubiquitously and cheaply available. But we have to keep in mind that new technologies in communications and media take years to diffuse, especially when they require significant infrastructure. It's true that local phone companies and cable operators have not rolled out service as quickly or widely as promised, and that new entrants have been quashed. On the other hand, penetration rates for high-speed services have shown healthy growth.

The FCC just released its third report on advanced telecommunications services, as mandated under the 1996 Telecommunications Act. The FCC found that high-speed services are being deployed in a "reasonable and timely manner." As of June 30, 2001, it found 9.6 million US high-speed subscribers, a 250-percent increase since the end of 1999. Seven percent of US households subscribe to high-speed services, according to the report.

But there's something odd about the FCC's data. The Commission defines broadband as delivering at least 200 kilobits in one direction, and "advanced communications services" as 200 kilobits or more in both directions. While this is a low enough bar to cover the cable modem and DSL services that make up the bulk of today's high-speed subscribers, it's disingenuous to call it broadband. (Always the clever marketer, AOL is running television ads trumpeting its "High Speed Broadband" service, which is no faster than any other cable modem or DSL offerings.)

Ten or 100 megabits, which could support true multimedia, fit the bill much more than what we have today, especially if the bandwidth is available in both directions. We're starting to see glimpses of what that could mean. For example, Moxi's home media server comes with a built-in 802.11a wireless transmitter (SEE **RELEASE 1.0**, NOVEMBER 2001), allowing it to stream video programming to multiple TVs in a home.

The longer view

If we really want to see broadband develop, we must have the courage of our convictions and the willingness to think medium-term. (Long-term, depending on how you define it, either we're all dead or we all have fiber to the Ethernet jacks in the back of our heads.) The best way to do so is through a portfolio of options. Specifically, we see four plausible long-range proposals for breaking the broadband impasse.Some should be pushed independently, regardless of how successful the others are. Some should be called into play under defined scenarios.

1. Split content and connectivity

The Internet fosters innovation because it's an open platform that separates connectivity from applications and content. Services on top of the network are decentralized to users, rather than built into the core. On the other hand, today's dominant broadband providers argue that they need revenues from services such as streaming video to justify their investment. They tie their high-speed Internet services to their control of last-mile pipes into homes.

A small but growing chorus of voices argues for breaking the linkage between connectivity and higher-level services or content. Commentators such as law professor Lawrence Lessig and technologists David Isenberg and Bob Frankston advocate policies that enforce this separation. There is talk, including an aborted proposal by state regulators in Pennsylvania, of splitting local phone companies into neutral last-mile connection providers and retail service providers. Such "loop divestiture" is a fairly drastic solution that would raise a host of operational, economic and policy challenges. It's too early to say that it's the right answer. But it gets at the real network architecture issues underlying the broadband bottleneck.

2. Open spectrum

An alterative path to ubiquitous broadband is to take service providers out of the equation entirely. Systems using unlicensed wireless connections can stitch together connectivity directly between network nodes. No one controls a network bottleneck, because the middle of the network is the shared capacity of the airwaves and the edges are commodity devices. As we explained in our open spectrum report (SEE **RELEASE 1.0**, NOVEMBER 2001), current unlicensed systems are limited, but the potential of this approach is extraordinary.

A combination of private and governmental efforts to develop open spectrum technologies and services could create an entirely new onramp to the broadband superhighway. The limitation of wireless technologies is that they are difficult to deploy ubiquitously, especially those that involve short-distance links. That hurdle can be overcome, but it will take a policy shift to allow unlicensed technologies to reach their full potential.

3. Man on the moon

In an October speech, former Intel ceo Andy Grove offered another alternative broadband recommendation. Government, he suggested, could fund research and development into potentially disruptive broadband technologies. As he put it, "What basically this amounts to is an idea or a proposal to fund a technology horse race; the goal being to respond to the 10x problem with a 10x change in technology effectiveness or cost effectiveness."

Grove's suggestion is to treat broadband like putting a man on the moon. President Kennedy set an aggressive goal, and the government provided the resources and road map to meet that goal. Plenty of breakthrough technology gets developed without government assistance, but the Internet itself is a famous case where market forces may not have produced an important innovation.

The broadband bottleneck isn't entirely a technology problem. Still, new technologies such as cheaper fiber-optics or better meshed wireless systems could change the game and create openings for new competitors.

4. Municipal and customer ownership

Finally, governments could become more active in seeing that broadband connections are available, just as they did to ensure the construction of highways after World War II. The interstate highway system was a federal program, but to date most government-sponsored communications infrastructure has been deployed at the municipal level. Several cities have built their own fiber backbones, which they lease to service providers and in some cases end-users on non-discriminatory terms. The "condominium fiber" model being tried in Canada is an offshoot of this approach (SEE **RELEASE 1.0**, JULY/AUGUST 2001).

As with open spectrum, the goal of government involvement would be to give users control over their own broadband connections, not to create a central state-run enterprise. Thinking about broadband as a utility is useful on some levels but not on others, because the economics of moving bits vary depending on the underlying architecture used.

Where are we going?

All these options have their downsides. They are worth considering because they crystallize the issues and escape the limitations of the current environment. Steps such as eliminating regulatory requirements on telephone companies or cable operators, even if justified, wouldn't alter the basic contours of the market.

It may be that no legal or regulatory changes are necessary. As we've described (SEE **RELEASE 1.0**, JULY/AUGUST 2001), several existing technologies could provide greater bandwidth to residential and business customers than current options. To get to market, though, they require service providers with the right incentives to deploy them. The current competitive and financial environment, in the US at least, makes the incumbent local telephone and cable operators the

COMING SOON

- PC Forum documentation.
- Bandwidth optimization.

- And much more. . . (If you know of any good examples of the categories listed above, please let us know.)

Resources & Contact Information

Kapi Attawar, **Endeavors Technology**, 1 (408) 973-9944; fax, 1 (408) 973-9593; kattawar@endeavors.com
Andrew Mahon, **Groove**, 1 (978) 720-2222; fax, 1 (978) 825-8377; amahon@groove.net
Frank Zvi, **Interwise**, 1 (408) 748-7800; frank@interwise.com
Jim Pflaging, **Intraspect**, 1 (650) 943-6000; fax, 1 (650) 938-4367; jimp@intraspect.com
Kittu Kolluri, **Neoteris**, 1 (650) 605-4800; kittu@neoteris.com
Stephen Hsu, **SafeWeb**, 1 (510) 601-8855; fax, 1 (510) 291-2893 hsu@safeweb.com
Bernard Hulme, **Tadpole Technology**, 44 (1223) 428-200; fax, 44 (1223) 428201; bernardh@tadpole.com
Michael Tanne, **XDegrees**, 1 (650) 691-0400; fax, 1 (650) 691-0490; mtanne@xdegrees.com

For further reading:

FCC Chairman Michael Powell, "'Digital Broadband Migration,'Part II",
http://www.fcc.gov/Speeches/Powell/2001/spmkp109.html
TechNet's broadband principles, http://www.technet.org/news/newsreleases/2002-01-15.64.pdf
FCC 3rd Report on the Availability of High-Speed and Advanced Telecommunications Capability,
http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-33A1.pdf
Bob Frankston, "Connectivity: What it is and Why it's so Important,"
http://www.satn.org/about/separateconnectivity.htm

dominant broadband providers. Most of them are still finishing their cable modem and DSL deployments.

The landscape is bound to change in the coming years, not least because of further consolidation. Long-distance phone companies, wireless operators and content owners without physical distribution (such as Disney and Viacom) are the odd men out in the current broadband game of musical chairs. They therefore have incentives to do more than sit still. What that will lead to is an open question. Other players, including content and application vendors such as Sony and Microsoft, may also have roles to play as broadband becomes more than just a way to surf the Web faster.

Internet 2.0 is still on the way. . . though it hasn't arrived yet. The broadband debate has moved from the periphery of communications policy to its center. Now would be a good time for those involved to stop complaining about what hasn't happened, and start talking about what *should* happen in the future. ■ **R 1.0**

Calendar of High-Tech Events

2002

MARCH 8-12	**SXSW INTERACTIVE** - Austin. TX. This offshoot of the South-by-Southwest independnt film festival offers heaping servings of online community, featuring thinkers, designers and Webloggers. For more information, call 1 (512) 467-7979; fax, 1 (512) 451-0754; email inter@sxsw.com. Register at www.sxsw.com/interactive.
MARCH 10-14	**ICANN MEETING** - Accra, Ghana. The Internet Corporation for Assigned Names and Numbers brings its work on Internet governance to Africa. More information will be available soon at www.icann.org. **E**
MARCH 13-20	**CEBIT 2002** - Hannover, Germany. The biggest European technology event, officially dubbed the World Business Fair for Office Automation, Information Technology and Telecommunications. For further information, call 49 (511) 89-0; www.cebit.de
MARCH 24-26	**PC FORUM** - Scottsdale, AZ. EDventure Holdings' premier conference, this year celebrating its 25th anniversary. Our theme is "Back to the Frontier," and our speakers include Craig Barrett (Intel), Jean-Marie Messier (Vivendi Universal), Joe Nacchio (Qwest), Steve Perlman (Moxi Digital), Hilary Rosen (RIAA) and Rick Belluzzo (Microsoft). Registration is now open at www.edventure.com/pcforum. **E** **K**
MARCH 25-29	**JAVA ONE** - San Francisco, CA. The world's largest developer conference and geekfest for Java developers. Hot topics will include Web services,wireless and handheld devices and emerging technologies. To register, call 1 (888) 886-8769; fax, 1 (781) 449-2674, or visit servlet.java.sun.com/javaone.
APRIL 16-19	**CFP2002**: The Twelfth Conference on Computers, Freedom & Privacy - San Francisco, CA. Continuing the debate on rights and wrongs in the online world. Speakers include California Attorney General Bill Lockyer, author Bruce Sterling and John Perry Barlow. For more information, email feedback@cfp2002.org. Register at www.cfp2002.org.
APRIL 20-25	**CHI 2002** - Minneapolis, MN. Leading international forum for the exchange of ideas and information about computer-human interaction. For information, contact CHI at 1 (410) 263-5382, or by email at chi2002-office@acm.org. www.acm.org/sigchi/chi2002
MAY 7-11	**WWW 2002** - Honolulu, HI. The Eleventh World Wide Web Conference, organized by the World Wide Web Consortium. For more information, email info@www2002.org. www.www2002.org

E Events Esther plans to attend.
K Events Kevin plans to attend.

Lack of a symbol is no indication of lack of merit. The full, current calendar is available on our Website, www.edventure.com. Please contact Irene Lawrence (irene@edventure.com) to let us know about other events we should include.

Back to the Frontier at the 25th PC Forum. Don't miss the year's most exceptional technology industry event! Join us – and your peers – to reinvigorate yourself for the challenges and opportunities ahead. Register today at **http://www.edventure.com/pcforum**!

Join the conversation. Subscribe to our free email newsletter, The conversation continues, for industry analysis and pointers. Sign up at **http://www.edventure.com/conversation/join.cfm**.

Release 1.0 Subscription Form

Complete this form and join the other industry executives who regularly rely on Release 1.0 to stay ahead of the headlines. Or if you wish, you can also subscribe online at www.release1-0.com.

Your annual Release 1.0 subscription costs **$795** per year (**$850** outside the US, Canada and Mexico), and includes both the print and electronic versions of 11 monthly issues; 25% off the cover price when you order from our online archives; a Release 1.0 binder; the bound transcript of this year's PC Forum (a $300 value) and an invitation to next year's PC Forum.

NAME ______________________________
TITLE ______________________________ COMPANY ______________________________
ADDRESS ______________________________
CITY ______________________________ STATE __________ ZIP __________ COUNTRY ______________
TELEPHONE ______________________________ FAX ______________________________
EMAIL* ______________________________ URL ______________________________
*personal email address required for electronic access.

☐ My colleagues should read Release 1.0, too!
Send me information about multiple copy subscriptions and electronic site licenses.

☐ Check enclosed ☐ Charge my (circle one): AMERICAN EXPRESS MASTER CARD VISA

CARD NUMBER ______________________________ EXPIRATION DATE ______________
NAME AND BILLING ADDRESS ______________________________
SIGNATURE ______________________________

Please fax this form to Natasha Felshman at 1 (212) 924-0240.

Payment must be included with this form. Your satisfaction is guaranteed or your money back.

If you wish to pay by check, please mail this form with payment to: EDventure Holdings, 104 Fifth Avenue, 20th Floor, New York, NY 10011, USA. If you have any questions, please call us at 1 (212) 924-8800; email us@edventure.com; www.edventure.com.